UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/047,193	01/15/2002	Lauri Paatero	9943-003US (2990568US/HM)	7915

570 7590 03/09/2005

AKIN GUMP STRAUSS HAUER & FELD L.L.P.
ONE COMMERCE SQUARE
2005 MARKET STREET, SUITE 2200
PHILADELPHIA, PA 19103-7013

EXAMINER	
CALLAHAN, PAUL E	

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 03/09/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/047,193	PAATERO, LAURI	
	Examiner	Art Unit	
	Paul Callahan	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *17 January 2002*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-8* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-8* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *17 January 2002* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 ~~or PTO/SB/08),~~ ~~Paper No(s)/Mail Date~~ _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-8 are pending in this application and have been examined.

Priority

2. Receipt is acknowledged of papers submitted under 35 U.S.C. 119(a)-(d), which papers have been placed of record in the file.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1, 2, 4, and 6-8 are rejected under 35 U.S.C. 103(a) as being unpatentable over Herve US 4,471,216, and Dolan et al., US 5,604,810.

As for claims 1, 2, and 4, Herve teaches a method of producing a response with a device (abstract) comprising; an input for receiving an input calculation means for producing a response which is responsive to the input and a secret key by utilizing a first predetermined function (col. 1 lines 60-67, col. 2 lines 1-10), and an output for feeding said response further (col. 2 lines 1-10), Dolan teaches the features of the claim not taught by Herve, namely; storing in a memory of the device a key-specific number and a coded key which is calculated by means of the secret key, the

key-specific number and a device-specific second predetermined function (col. 3 lines 65-67, col. 4 lines 1-18), and, when producing the response reading said key-specific number and coded key from the memory, calculating the secret key on the basis of said key-specific number and coded key by using the inverse function of said second predetermined function, and utilizing the calculated secret key to produce said response (col. 4 lines 1-15). Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate this feature of Dolan et al. into the system of Herve. Motive to make this combination is found for example in col. 2 lines 10-20 of Dolan where the advantage of allowing smart-card authentication without revealing a secret key to a server is discussed.

1-2 & 4 (AK)

As for claims 6-8, these claims represent the apparatus carrying out the method of claims ~~1-5~~ and are therefore rejected on the same basis as those claims.

5. Claims 3 and 5 are rejected under 35 U.S.C. 103(a) as being unpatentable over Herve and Dolan as applied to claims 1 and 4 above, and further in view of Kocher, International Publication Number: WO 99/35782.

As for claim 3, the combination of Herve and Dolan fails to teach the method as claimed in claim 1, characterized by calculating and storing in the memory of the device a new coded key and a new key-specific number when the calculation means have utilized said first predetermined function a predetermined number of times. However Kocher does teach this feature (page 8 lines 25-33). Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate this feature of Kocher into the system of Herve and Dolan. It would have been desirable to do so as this would increase the security of key storage.

As for claim 5, the combination of Herve and Dolan fails to teach the device as claimed in claim 4, characterized in that the device comprises; coding means for calculating a new coded key by means of the secret key a new key-specific number to be fed to the coding means, and said second predetermined function, and that the device comprises means for replacing the coded key and the key-specific number stored in the memory with the new coded key calculated by the coding means, and the new key-specific number. However Kocher does teach these features (page 8 lines 25 through page 9 line 15). Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate this feature of Kocher into the system of Herve and Dolan. It would have been desirable to do so as this would increase the security of key storage.

Conclusion

6. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Paul E. Callahan whose telephone number is (571) 272-3869. The examiner can normally be reached on M-F from 9 to 5.

If attempts to reach the examiner by telephone are unsuccessful, the Examiner's supervisor, Andrew Caldwell, can be reached on (571) 272-3868. The fax phone number for the organization where this application or proceeding is assigned is: (703) 872-9306. Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.

3/5/05
Paul Callahan

Andrew Caldwell
ANDREW CALDWELL
SUPERVISORY PATENT EXAMINER